# PATENT COOPERATION TREATY

# PCT



## INTERNATIONAL PRELIMINARY REPORT ON PATENTABILITY
(Chapter II of the Patent Cooperation Treaty)

(PCT Article 36 and Rule 70)

| Applicant's or agent's file reference | FOR FURTHER ACTION | See Form PCT/IPEA/416 |
|---|---|---|
| International application No. PCT/US05/01098 | International filing date *(day/month/year)* 11 January 2005 (11.01.2005) | Priority date *(day/month/year)* 15 January 2004 (15.01.2004) |
| International Patent Classification (IPC) or national classification and IPC IPC(7): G06F 11/30 and US Cl.: 713/200 | | |
| Applicant SONG, JUN | | |

1. This report is the international preliminary examination report, established by this International Preliminary Examining Authority under Article 35 and transmitted to the applicant according to Article 36.
2. This REPORT consists of a total of 7 sheets, including this cover sheet.
3. This report is also accompanied by ANNEXES, comprising:
   a. ☒ *(sent to the applicant and to the International Bureau)* a total of 9 sheets, as follows:
      ☒ sheets of the description, claims and/or drawings which have been amended and are the basis of this report and/or sheets containing rectifications authorized by this Authority (see Rule 70.16 and Section 607 of the Administrative Instructions).
      ☐ sheets which supersede earlier sheets, but which this Authority considers contain an amendment that goes beyond the disclosure in the international application as filed, as indicated in item 4 of Box No. I and the Supplemental Box.
   b. ☐ *(sent to the International Bureau only)* a total of (indicate type and number of electronic carrier(s)) _____ , containing a sequence listing and/or tables related thereto, in electronic form only, as indicated in the Supplemental Box Relating to Sequence Listing (see Section 802 of the Administrative Instructions).
4. This report contains indications relating to the following items:
   - ☒ Box No. I Basis of the report
   - ☐ Box No. II Priority
   - ☐ Box No. III Non-establishment of opinion with regard to novelty, inventive step and industrial applicability
   - ☐ Box No. IV Lack of unity of invention
   - ☒ Box No. V Reasoned statement under Article 35(2) with regard to novelty, inventive step or industrial applicability; citations and explanations supporting such statement
   - ☐ Box No. VI Certain documents cited
   - ☐ Box No. VII Certain defects in the international application
   - ☐ Box No. VIII Certain observations on the international application

| Date of submission of the demand | Date of completion of this report |
|---|---|
| 09 August 2005 (09.08.2005) | 24 October 2005 (24.10.2005) |
| Name and mailing address of the IPEA/US<br>Mail Stop PCT, Attn: IPEA/US<br>Commissioner for Patents<br>P.O. Box 1450<br>Alexandria, Virginia 22313-1450<br>Facsimile No. (703) 305-3230 | Authorized officer Lisa Vieu<br>Ayaz R Sheikh<br>Telephone No. 571-272-2100 |

INTERNATIONAL PRELIMINARY REPORT ON PATENTABILITY

International application No.
PCT/US05/01098

**Box No. I Basis of the report**

1. With regard to the **language**, this report is based on:

☐ the international application in the language in which it was filed.

☐ a translation of the international application into English, which is the language of a translation furnished for the purposes of:

☐ international search (under Rules 12.3 and 23.1(b))

☐ publication of the international application (under Rule 12.4(a))

☐ international preliminary examination (under Rules 55.2(a) and/or 55.3(a))

2. With regard to the **elements** of the international application, this report is based on *(replacement sheets which have been furnished to the receiving Office in response to an invitation under Article 14 are referred to in this report as "originally filed" and are not annexed to this report)*:

☐ the international application as originally filed/furnished

☒ the description:
pages 1 - 41 as originally filed/furnished
pages* NONE received by this Authority on
pages* NONE received by this Authority on

☒ the claims:
pages NONE as originally filed/furnished
pages* NONE as amended (together with any statement) under Article 19
pages* 42-47, 47/1 and 48 received by this Authority on 09 August 2005 (08.08.2005)
pages* NONE received by this Authority on

☒ the drawings:
pages 1/14 - 12/14 as originally filed/furnished
pages* 13/14 and 14/14 received by this Authority on 09 August 2005 (09.08.2005)
pages* NONE received by this Authority on

☐ a sequence listing and/or any related table(s) - see Supplemental Box Relating to Sequence Listing.

3. ☐ The amendments have resulted in the cancellation of:

☐ the description, pages
☐ the claims, Nos.
☐ the drawings, sheets/figs
☐ the sequence listing (*specify*):
☐ any table(s) related to the sequence listing (*specify*):

4. ☐ This report has been established as if (some of) the amendments annexed to this report and listed below had not been made, since they have been considered to go beyond the disclosure as filed, as indicated in the Supplemental Box (Rule 70.2(c)).

☐ the description, pages
☐ the claims, Nos.
☐ the drawings, sheets/figs
☐ the sequence listing (*specify*):
☐ any table(s) related to the sequence listing (*specify*):

* *If item 4 applies, some or all of those sheets may be marked "superseded."*

INTERNATIONAL PRELIMINARY REPORT ON PATENTABILITY

International application No.
PCT/US05/01098

**Box No. V Reasoned statement under Article 35(2) with regard to novelty, inventive step or industrial applicability; citations and explanations supporting such statement**

1. Statement

| | | |
|---|---|---|
| Novelty (N) | Claims 1-29 | YES |
| | Claims none | NO |
| Inventive Step (IS) | Claims NONE | YES |
| | Claims 1-29 | NO |
| Industrial Applicability (IA) | Claims 1-29 | YES |
| | Claims NONE | NO |

2. Citations and Explanations (Rule 70.7)
Please See Continuation Sheet

Supplemental Box

In case the space in any of the preceding boxes is not sufficient.

Continuation of:

V. 2. Citations and Explanations:
Claim 1 lacks novelty under PCT Article 33(2) as being anticipated by Dick (US Patent Publication 2003/0217290 A1).

Regarding claim 1, Dick teaches a request-response based transactional auditing method for providing a centralized transactional real-time adaptive identity-driven audit trail over a processing device or sequence of processing devices connected by wired or wireless networks, said method comprising the steps of:

selecting a communication protocol for transmitting a message from a first processing device to a second processing device in a transaction beginning with an incoming request and ending with an outgoing response to the incoming request (paragraph 0048);

creating at least one audit-request object having audit data (paragraph 0042);

embedding the audit-request object into the incoming request when the incoming request is in compliance with the communication protocol used downstream during a request process (paragraph 0042);

creating at least one audit-response object at the start of a response process, said audit-response object having audit data (paragraph 0062);

embedding an audit-response object in an outgoing response, said outgoing response being in compliance with the communication protocol upstream during the response process (paragraph 0062);

moving the request and the response through a transaction (paragraph 0043).

Claims 2-4 lack an inventive step under PCT Article 33(3) as being obvious over Dick (US Patent Publication 2003/0217290 A1) in view of Schaefer et al. (US Patent Publication 2002/0010867 A1).

Regarding claim 2, Dick teaches further comprising the steps of:

adding the Transaction ID to the audit-request object (paragraph 0062);

verifying the audit-response object contains the Transaction ID (paragraph 0062);

altering at least part of the audit data carried in the audit-request object or audit-response object at desired points during the transaction (figure 5, reference number 168);

saving at least part of the audit data which contains at least the transaction id in the audit-request object and the audit-response object in persistence storage at desired points of the transaction (figure 5, reference number 170), and

removing the audit-response object from the outgoing response object before the outgoing response object leaves the transaction entry point (paragraph 0047).

**Supplemental Box**

whereby the Transaction ID, audit-request object and audit-response object may be used to identify the transaction and log the events during the transaction at any point in order to provide a centralized transactional real-time adaptive identity-driven audit trail that enables the collection and removal of the event trail log for the transaction, and allowing persistence of the audit data of the audit-request object and audit-response object at the centralized user trail repository (paragraph 0046 and 0060, figure 3, reference number 100).

Dick does not teach creating a unique Transaction ID for said transaction. Schaefer et al. teaches creating a unique Transaction ID for said transaction (paragraph 0077).

Regarding claim 3, Dick as modified by Schaefer et al. teaches further comprising the step of representing the audit-request object and the audit-response object by XML (see paragraph 0028 of Schaefer et al.).

Regarding claim 4, Dick as modified by Schaefer et al. teaches further comprising the step of keeping the audit data of the audit-request object and the audit-response object in an encrypted form during the transaction so that the audit data can be securely transmitted when desired (see figure 6, reference number 196 of Dick).

Claims 5-29 lack an inventive step under PCT Article 33(3) as being obvious over Dick (US Patent Publication 2003/0217290 A1) in view of Schaefer et al. (US Patent Publication 2002/0010867 A1), and further in view of Eibach et al. (US Patent Publication 2003/0084350 A1).

Regarding claim 5, Dick as modified by Schaefer et al. teaches all the limitations of claims 1-3, above. However, Dick as modified by Schaefer et al. does not teach further comprising the steps of: passing downstream said audit-request object by means of at least one HTTP header; and passing upstream said audit-response object by means of at least one HTTP header.

Eibach et al. teaches further comprising the steps of: passing downstream said audit-request object by means of at least one HTTP header (paragraph 0018); and passing upstream said audit-response object by means of at least one HTTP header (paragraph 0018).

Regarding claim 6, Dick as modified by Schaefer et al./Eibach et al. teaches said audit-data contains user Id (see paragraph 0055 of Dick).

Regarding claim 7, Dick as modified by Schaefer et al./Eibach et al. teaches said audit-data contains session Id (see paragraph 0025 of Eibach et al.).

Regarding claim 8, Dick as modified by Schaefer et al./Eibach et al. teaches said audit-data contains one or more fields selected from the group consisting of user registry domain, remote connection host, remote connection ip address, roles assigned to the user, any other user related information like user account number (see paragraph 0023 of Eibach et al.).

Regarding claim 9, Dick as modified by Schaefer et al./Eibach et al. teaches the audit-data contains TGT which contains transaction id, user id, token expiration time, and authorized roles for the user (see paragraph 0077 of Schaefer et al. and paragraphs 0055 & 0060 of Dick).

Regarding claim 10, Dick as modified by Schaefer et al./Eibach et al. teaches the audit-data contains one or more fields selected from the group consisting of policy fields: resource that needs to be protected, roles that specify if the user is allowed or denied for access this resource, rules that associate the user with the resource and the roles to decide who can access the said resource (see paragraph 0013 of Schaefer et al.).

Regarding claim 11, Dick as modified by Schaefer et al./Eibach et al. teaches audit-data contains one or more fields selected from the group consisting of audit trail fields: service id, authorization status, failed reason, accessing role, service accessing time, log-info (see paragraph 0056 of Schaefer et al.).

Regarding claim 12, Dick as modified by Schaefer et al./Eibach et al. teaches said audit-data contains one or more fields selected from the group consisting of lifespan fields: Transaction Creation Time, Transaction expiration-time, Transaction time out (see paragraph 0060 of Dick).

Regarding claim 13, Dick as modified by Schaefer et al./Eibach et al. teaches further comprising the steps of loading security policies into memory in cached form (see paragraph 0023 of Eibach et al.).

Regarding claim 14, Dick as modified by Schaefer et al./Eibach et al. teaches further comprising the steps of adding the policies associated with the resources requested for access to audit-data (see paragraph 0062 of Dick).

Regarding claim 15, Dick as modified by Schaefer et al./Eibach et al. teaches further comprising the steps of:
authenticating a user (see paragraph 0061 of Dick), and
authorizing a user for a given resource (see paragraph 0061 of Dick).

Supplemental Box

Regarding claim 16, Dick as modified by Schaefer et al./Eibach et al. teaches further comprising the steps of:
authenticating a user in said first device against user registry (see paragraph 0061 of Dick);
adding authentication event log data into audit-data (see paragraph 0023 of Eibach et al.);
creating a encrypted TGT token of said user (see paragraph 0055 & 0063 of Dick);
adding TGT token into audit-data (see paragraph 0063 of Dick);
forwarding the audit-data containing TGT token to the said first processing device and then said second processing device handling authorization process, said audit-data containing said TGT token facilitating processing of subsequent requests (see paragraph 0063 of Dick);
returning TGT token to the requesting-client as a ticket for the next time access with the associated session id (see paragraph 0063 of Dick).

Regarding claim 17, Dick as modified by Schaefer et al./Eibach et al. teaches further comprising the steps of:
obtaining TGT token from audit-data (see figure 5, reference number 172 of Dick),
decrypting TGT token to verify the user and retrieve the following (see paragraph 0055 of Dick): user id, token expiration time, roles assigned to said user, other relevant information stored within TGT token (see paragraph 0077 of Schaefer et al. and paragraphs 0055 & 0060 of Dick),
retrieving the policies associated with the resources for access from either policy store, in memory cache or audit-data (see figure 6A, step number 4 of Eibach et al.);
authorizing said user based on said TGT token and said policies retrieved (see paragraph 0076 of Schaefer et al.),
adding the authorization event log into said audit data (see paragraph 0023 of Eibach et al.),
granting or denying resources access based on authorization status (see paragraph 0076 of Schaefer et al.),
forwarding the audit-data containing TGT token said second processing device handling authorization process, said audit-data containing said TGT token facilitating processing of subsequent requests (see paragraph 0063 of Dick).

Regarding claim 18, Dick as modified by Schaefer et al./Eibach et al. teaches wherein said first processing device is a proxy server and wherein said method further comprises the step of adding a module to said proxy server, the module adapted to allow dynamic loading of an in-bound filter and an out-bound filter that enable the proxy server to process a HTTP request before sending the request to a resource and to process a response before returning the response (see paragraph 0031 of Eibach et al.).

Regarding claim 19, Dick as modified by Schaefer et al./Eibach et al. teaches further comprising the steps of obtaining user profile for a user (see paragraph 0045 of Eibach et al.).

Regarding claim 20, Dick as modified by Schaefer et al./Eibach et al. teaches further comprising the steps of:
authenticating said user based on authentication and authorization API by a API vendor (see paragraph 0022 of Eibach et al.), and
authorizing said user for a given resource based on said API (see paragraph 0013 of Schaefer et al.).

Regarding claim 21, Dick as modified by Schaefer et al./Eibach et al. teaches further comprising the steps of:
validating data in the request (see paragraph 0044 of Eibach et al.);
checking data integrity (see paragraph 0044 of Eibach et al.).

Regarding claim 22, Dick as modified by Schaefer et al./Eibach et al. teaches further comprising the steps of performing XML transformation (see paragraph 0047 of Eibach et al.).

Regarding claim 23, Dick as modified by Schaefer et al./Eibach et al. teaches wherein said first processing device and said second processing device are connected via the internet so that web services are transfer requests and responses between said first processing device and said second processing device (see figure 2 of Eibach et al.), and wherein the audit data is added to the audit-request object and the audit-response object regarding activities of web services by the identify of the user and not by the identity of the web services (see paragraph 0055 of Dick).

Regarding claim 24, Dick as modified by Schaefer et al./Eibach et al. teaches further comprising the steps of:
inserting said audit-data via SOAP message (see abstract of Eibach et al. paragraph 0035 of Schaefer et al.),
convert SOAP message form of audit-data from response to other forms and moving upstream (see paragraph 0035 of Schaefer et al.).

Regarding claim 25, Dick as modified by Schaefer et al./Eibach et al. teaches further comprising the steps of:
perform data-binding to transfer business data into audit trail based on the security rules specified in XSL (see paragraph 0023of Eibach et al.).

Regarding claim 26, Dick as modified by Schaefer et al./Eibach et al. teaches further comprising the steps of:
passing downstream said audit-request object by means of at least one JMS header (see paragraph 0018 of Eibach et al.); and
passing upstream said audit-response object by means of at least one JMS header (see paragraph 0018 of Eibach et al.).

**Supplemental Box**

Regarding claim 27, Dick as modified by Schaefer et al./Eibach et al. teaches further comprising the steps of:
using the persisted audit data to create enterprise data replica for system fail over to provide business continuity (see paragraph 0042 of Dick).

Regarding claim 28, Dick as modified by Schaefer et al./Eibach et al. teaches further comprising the steps of:
retrieving security policy from audit data (see paragraph 0077 of Schaefer et al.); and
authorizing user resource access based on the security policy for authorization points located at desired location to provide multi-tiered authorization (see paragraph 0061 of Dick).

Regarding claim 29, Dick as modified by Schaefer et al./Eibach et al. teaches further comprising the steps of:
retrieving security policy from audit data (see paragraph 0077 of Schaefer et al.); and
authorizing user resource access based on the security policy for authorization points located at desired location to provide multi-tiered authorization (see paragraph 0061 of Dick).
---------- NEW CITATIONS ----------